REMARKS

The present Amendment amends claims 9, 21 and 33 and leaves claims 10-12, 22-24 and 34-36 unchanged. Therefore, the present application has pending claims 9-12, 21-24 and 33-36.

Amendments were made to the Abstract so as to clarify the description of the present invention. Entry of these amendments is respectfully requested.

Applicants note that the Examiner did not consider the references cited by an Information Disclosure Statement submitted on March 28, 2001 along with the present application. A copy of said Information Disclosure Statement is attached herewith. An indication that the references cited therein have been considered is respectfully requested.

Claims 9 and 10 stand rejected under 35 USC §103(a) as being unpatentable over Coppersmith (U.S. Patent No. 6,189,095) in view of Djakovic (U.S. Patent No. 6,351,539); claims 11 and 12 stand rejected under 35 USC §103(a) as being unpatentable over Coppersmith in view of Djakovic and further in view of Wasilewski (U.S. Patent No. 6,424,714); claims 21 and 22 stand rejected under 35 USC §103(a) as being unpatentable over Coppersmith in view of Djakovic; claims 23 and 24 stand rejected under 35 USC §103(a) as being unpatentable over Coppersmith in view of Djakovic and further in view of Wasilewski; claims 33 and 34 stand rejected under 35 USC §103(a) as being unpatentable over Coppersmith in view of Djakovic; and claims 35 and 36 stand rejected under 35 USC §103(a) as being unpatentable over Coppersmith in view of Djakovic and further in view of Wasilewski. These rejections

are traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in claims 9-12, 21-24 and 33-36 are not taught or suggested by Djakovic, Coppersmith and Wasilewski whether taken individually or in combination with each other as suggested by the Examiner. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw these rejections.

Amendments were made to each of independent claims 9, 21 and 33 from which the other claims depend so as to more clearly describe features of the present invention. Particularly, amendments were made to the claims so as to more clearly recite that the present invention provides a symmetric key decryption, method, apparatus and medium for storing a program.

According to the present invention, ciphertext is divided so as to generate a plurality of ciphertext blocks each having a predetermined length, a random number sequence is generated based on a secret key, and a random number block is generated corresponding to one of the ciphertext blocks from the random number sequence.

Unique according to the present invention is that a feedback value, obtained a result of operation on one of the ciphertext blocks and the random number block, is output so that the feedback value can be fed back for use in the operation on another one of the ciphertext blocks. As per the present invention, a decryption operation is performed using the one ciphertext block, the random number block and the fed back value so as to produce a plaintext block.

Thus, by use of the present invention after dividing a ciphertext into a plurality of ciphertext blocks, an arithmetic operation result of one ciphertext block is applied to the arithmetic operation of another ciphertext block. This feature of the present invention is illustrated, for example, in Fig. 11 as F1', F2' and F3'.

The above described features of the present invention now more clearly recited in the claims are not taught or suggested by any of the references of record whether taken individually or in combination with each other. Particularly the above described features of the present invention are not taught or suggested by Djakovic or Coppersmith whether taken individually or in combination with each other as suggested by the Examiner.

Djakovic teaches a decryptor mechanism as illustrated, for example, in Fig. 3 thereof. As taught by Djakovic, a block decipher mechanism decrypts a ciphertext block into a plain text block. Djakovic further teaches that the decryption operation thereof is limited to the processing of a single ciphertext block, for example, as illustrated in Fig. 3. However, at no point is there any teaching or suggestion in Djakovic where the output result of an operation performed on a first ciphertext block is used for performing an operation on a succeeding ciphertext block as in the present invention. There is no such teaching of the above described features of the present invention as recited in the claims in Djakovic contrary to the allegations by the Examiner.

In the Office Action the Examiner alleges that Djakovic teaches the feedback mechanism, for example, in col. 2, lines 26-36, wherein it describes that:

> "the second block cipher mechanism takes as input the output of the exclusive-or mechanism and produces a

second enciphered output based on the output of the exclusive-or mechanism and on a second key".

The above described teachings of Djakovic are not in anyway related to the generation of a feedback value from an operation on a first ciphertext block, wherein the feedback value is fed back for use in an operation on another ciphertext block as in the present invention as recited in the claims. Djakovic merely teaches a feed forward process wherein, for example, as illustrated in Fig. 3 a first block decipher 20-1 performs an operation and the output of said operation is fed forward to the exclusive-or 24-1. The exclusive-or 24-1 combines a random number and the output of the first block decipher 20-1 and further feeds forward the output thereof to the second block decipher 18-1. As per Djakovic the random number supplied to the exclusive-or 24-1 is generated by a third block decipher 22-1 which has input thereto an enciphered random number. The output from the second block decipher 18-1 is provided as an output stream.

At no point is there any teaching or suggestion in Djakovic of a feedback operation as that term is understood by those of ordinary skill in the art. Djakovic simply teaches feed forward processing without returning a result of one processing on first data back so said result can be used in a same processing on another data as in the present invention.

The above described deficiencies of Djakovic are not supplied by any of the other references of record particularly Coppersmith and Wasilewski. Therefore, combining the teachings of Djakovic, Coppersmith and Wasilewski in the manner suggested by the Examiner in the Office Action still fails to teach or suggest the features of the present invention as now more clearly recited in the claims.

Coppersmith merely discloses a block decipher technique that uses three or more transformation stages for decrypting a ciphertext block wherein each stage includes a plurality of rounds. The Examiner's attention is directed to, for example, Figs. 3 and 4 and col. 20, lines 7-10 of Coppersmith. In the block decipher mechanism of Coppersmith, a decryption result of one ciphertext block is not fed back and used to effect decryption of another ciphertext block. Coppersmith simply divides a ciphertext block into a plurality of words as illustrated in Fig. 4 and as discussed on col. 18, line 10 through col. 19, line 54 thereof. Fig. 4 of Coppersmith teaches that an operation result of one word is fed forward affecting the operation on other words. Thus, in Coppersmith a decryption operation proceeds with a plurality of words affecting each other in a feed forward manner. However, this operation as taught by Coppersmith is not a feedback of an output result of a preceding operation on a first set of data for use in the same operation on a second set of data as that term is understood by those of ordinary skill in the art and as recited in the claims.

In the present invention as recited in the claims, the feedback provides that an operation producing a decryption result of a ciphertext block C_i affects the same operation producing a decryption result of another ciphertext block C_j. However, the reverse does not occur namely, the decryption result of the block C_j is not used to affect the decryption result of the ciphertext C_i.

Thus, Djakovic and Coppersmith fail to teach or suggest outputting a feedback value obtained as a result of operation on the one ciphertext block and the random number blocks, wherein the feedback value is fed back for use in the operation of another one of the ciphertext blocks and performing a decryption

operation using the one ciphertext block, the random number block and the feedback value obtained as a result of operation of still another one of the ciphertext blocks to produce a plain text block as recited in the claims.

The above noted deficiencies of Djakovic and Coppersmith are also evident in Wasilewski. Therefore combining the teachings of Djakovic, Coppersmith and Wasilewski in the manner suggested by the Examiner in the Office Action would still fail to teach or suggest the features of the present invention as recited in the claims.

Wasilewski was merely relied upon by the Examiner for an alleged teaching of extracting secret data and checking the redundancy data and the secret data to detect whether the ciphertext has been altered.

However, there is no teaching or suggestion in Wasilewski of outputting a feedback value obtained as a result of operation on the one ciphertext block and the random number blocks, wherein the feedback value is fed back for use in the operation of another one of the ciphertext blocks and performing a decryption operation using the one ciphertext block, the random number block and the feedback value obtained as a result of operation of still another one of the ciphertext blocks to produce a plain text block as recited in the claims.

Therefore, as is quite clear from the above, the features of the present invention as now more clearly recited in the claims are not taught or suggested by Djakovic, Coppersmith or Wasilewski whether taken individually or in combination with each other as suggested by the Examiner. Accordingly, reconsideration and withdrawal of the 35 USC §103(a) rejections of claims 9-12, 21-24 and 33-36 as

being unpatentable over Djakovic in view of Coppersmith, and over Djakovic in view of Coppersmith and further in view of Wasilewski is respectfully requested.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references utilized in the rejection of claims 9-12, 21-24 and 33-36.

In view of the foregoing amendments and remarks, applicants submit that claims 9-12, 21-24 and 33-36 are in condition for allowance. Accordingly, early allowance of claims 9-12, 21-24 and 33-36 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (520.39632VX1).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 684-1120